(12) UK Patent Application (19) GB (11) 2 323 757 (13) A

(43) Date of A Publication 30.09.1998

(21) Application No 9803074.5

(22) Date of Filing 16.02.1998

(30) Priority Data
(31) 08828449 (32) 28.03.1997 (33) US

(71) Applicant(s)
International Business Machines Corporation
(Incorporated in USA - New York)
Armonk, New York 10504, United States of America

(72) Inventor(s)
Joseph M Crichton
Peter F Garvin
Jeffrey W Staten
Waaiki L Wright

(74) Agent and/or Address for Service
G M Zerbi
IBM United Kingdom Limited, Intellectual Property Department, Mail Point 110, Hursley Park, WINCHESTER, Hampshire, SO21 2JN, United Kingdom

(51) INT CL[6]
H04L 29/06

(52) UK CL (Edition P)
H4P PPEB

(56) Documents Cited
GB 2318031 A GB 2317539 A EP 0743777 A2
EP 0713311 A1 WO 98/18248 A1 WO 97/16911 A1

(58) Field of Search
UK CL (Edition P) H4P PPA PPEB PPEC
INT CL[6] H04L 9/00 12/22 12/46 12/66 29/06 29/08
Online : WPI, INSPEC

(54) Abstract Title
Lightweight secure communication tunnelling over the internet

(57) A lightweight secure tunnelling protocol or LS rP permits communicating across one or more firewalls by using a middle server or proxy. Three proxies are used to establish an end-to-end connection that navigates through the firewalls. In a typical configuration, a server 211 is behind a first firewall 23 and a client 222 behind a second firewall 25 are interconnected by an untrusted network 12 (e.g., the Internet) between the firewalls. A first inside firewall SOCKS-aware server-side end proxy 213 connects to the server 211 inside the first firewall 23. A second inside firewall SOCKS-aware client-side end Proxy 223 is connected to by the client 222 inside the second firewall 25. Both server-side and client-side end proxies 213, 223 can address a third proxy (called a middle proxy) 26 outside the two firewalls 23, 25.

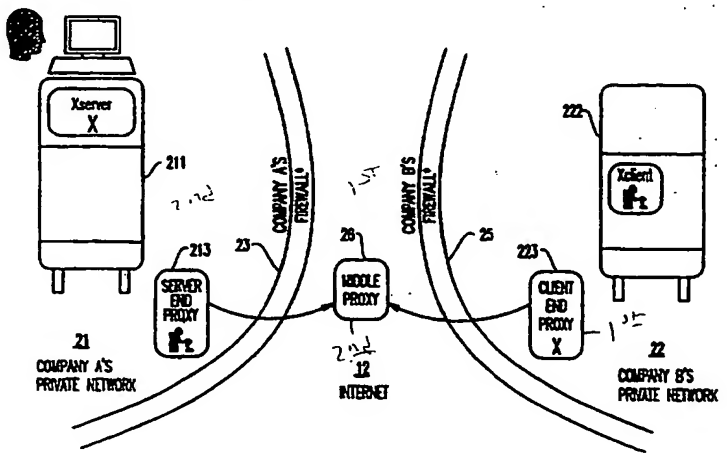


FIG.4

GB 2 323 757 A

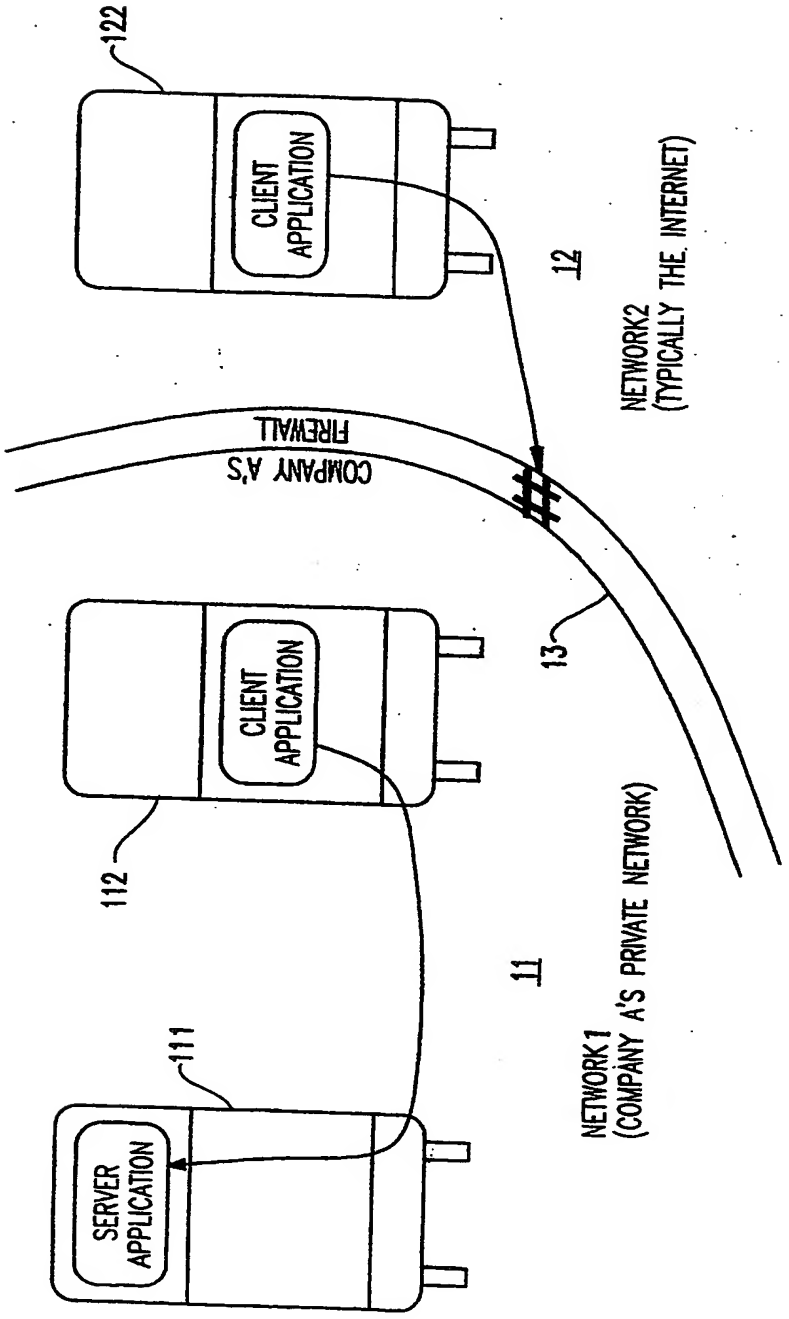

122
CLIENT APPLICATION
12
NETWORK2
(TYPICALLY THE INTERNET)
COMPANY A'S FIREWALL
13
CLIENT APPLICATION
112
11
NETWORK1
(COMPANY A'S PRIVATE NETWORK)
111
SERVER APPLICATION

FIG.1

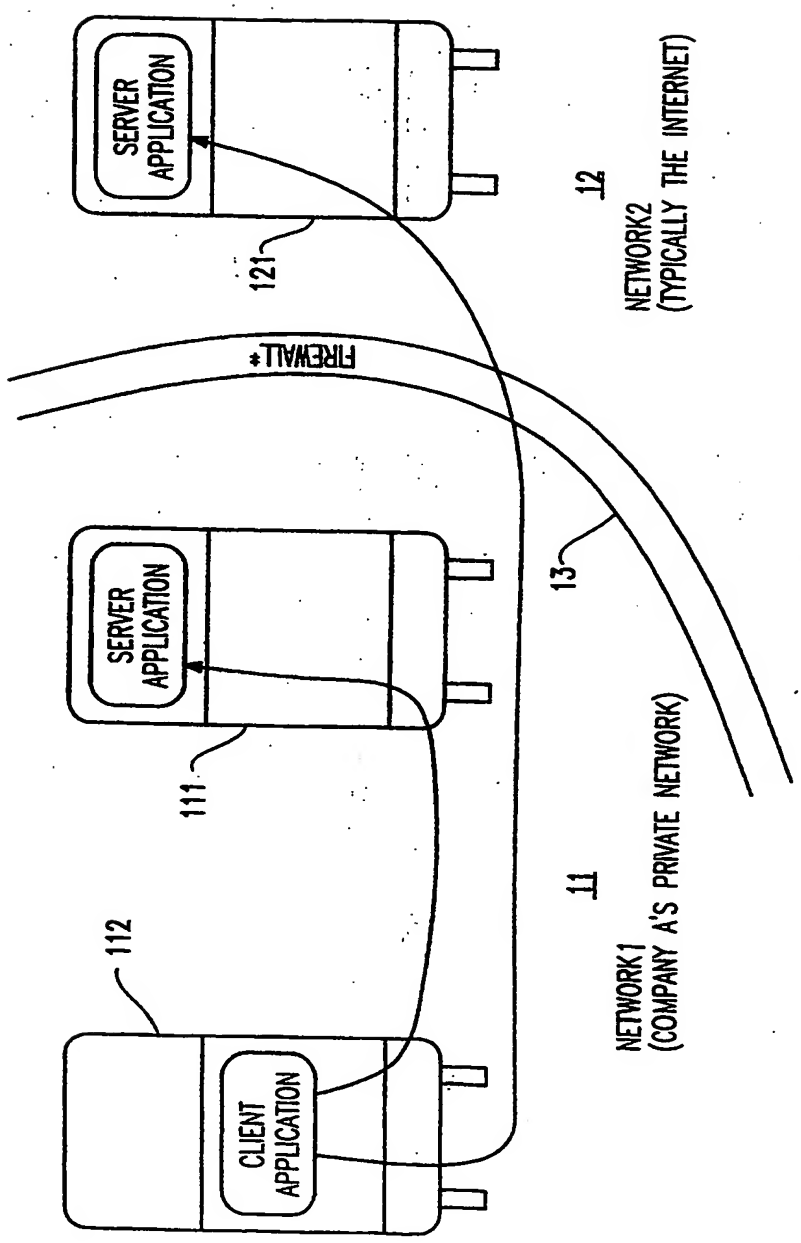


FIG.2

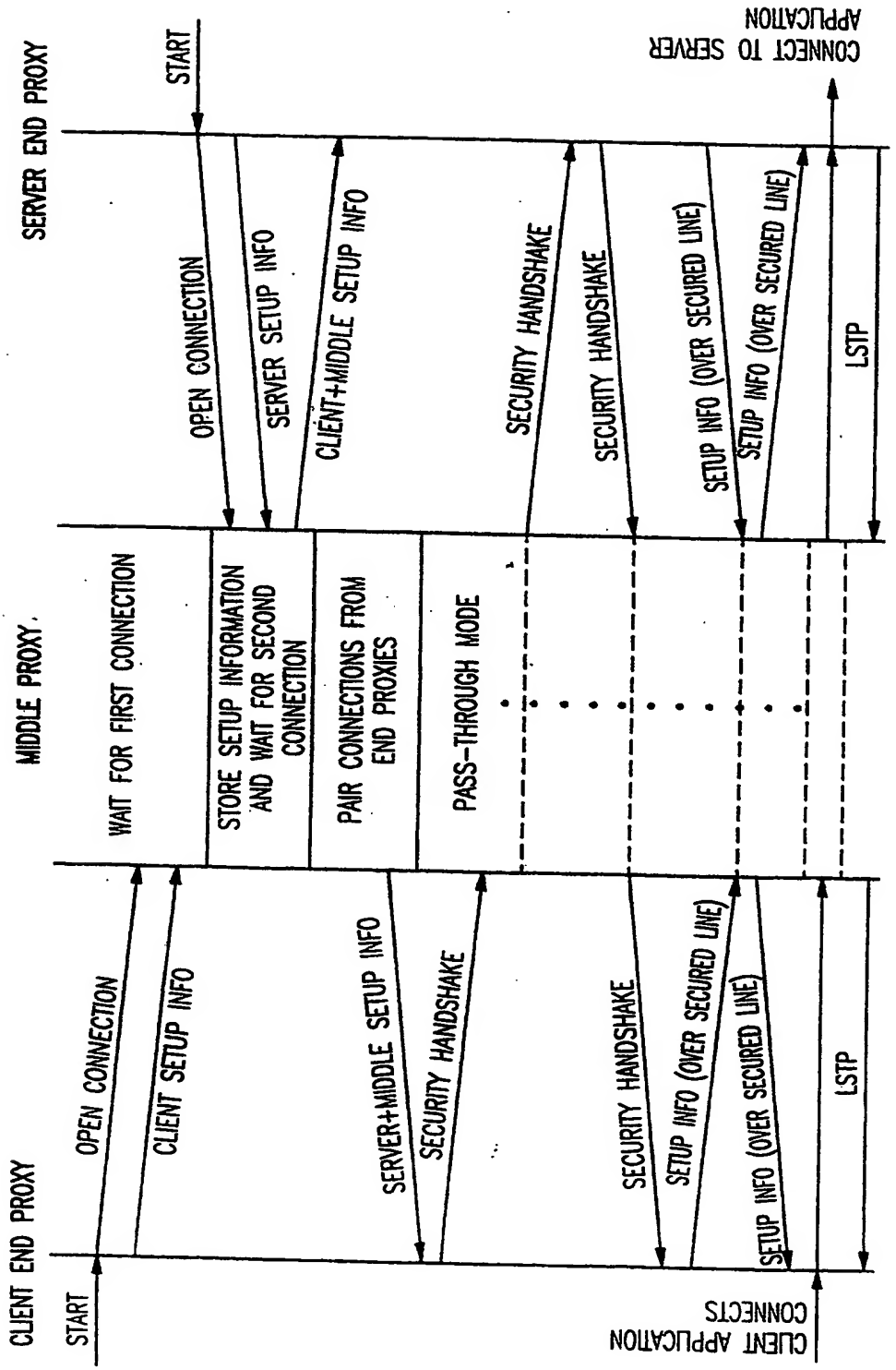


FIG.5

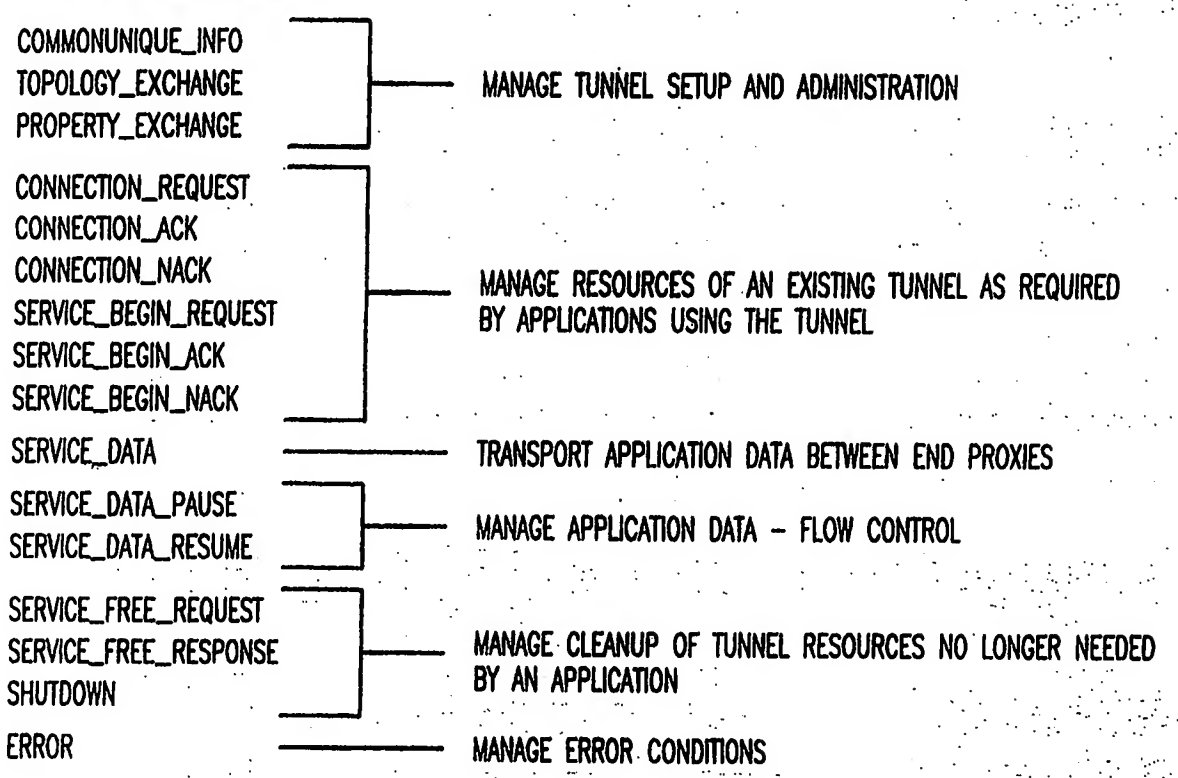


FIG.6

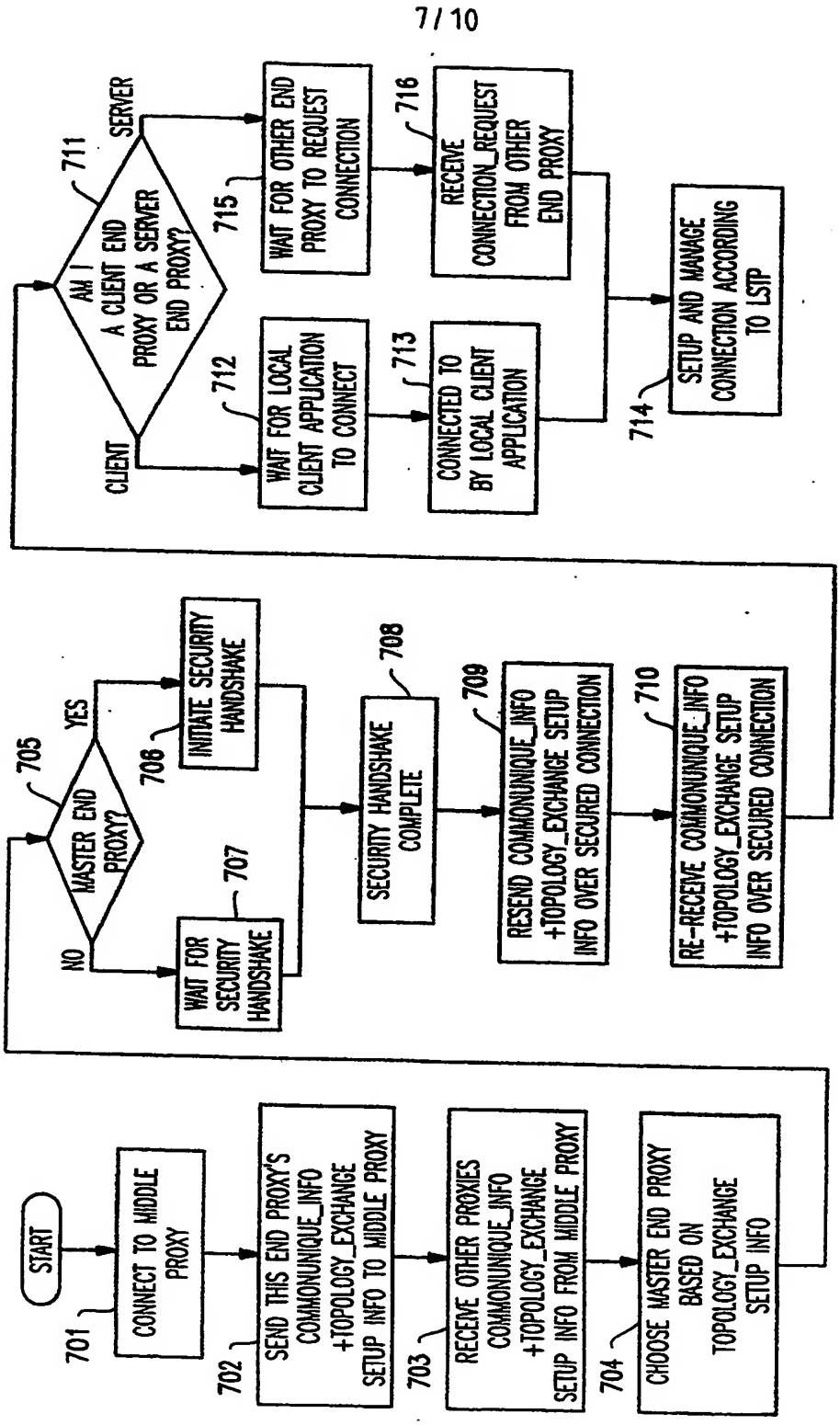
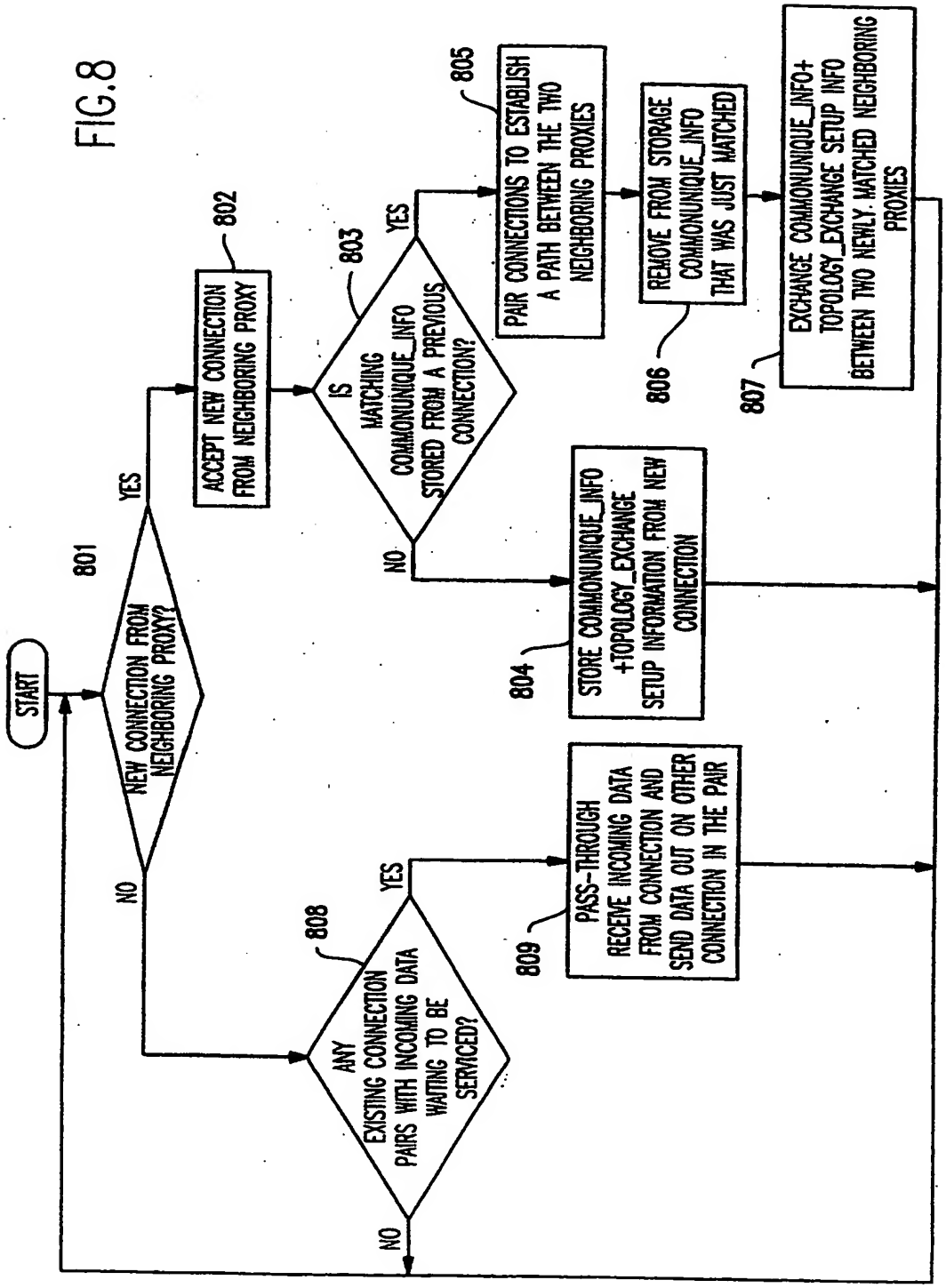


FIG.7

FIG.8



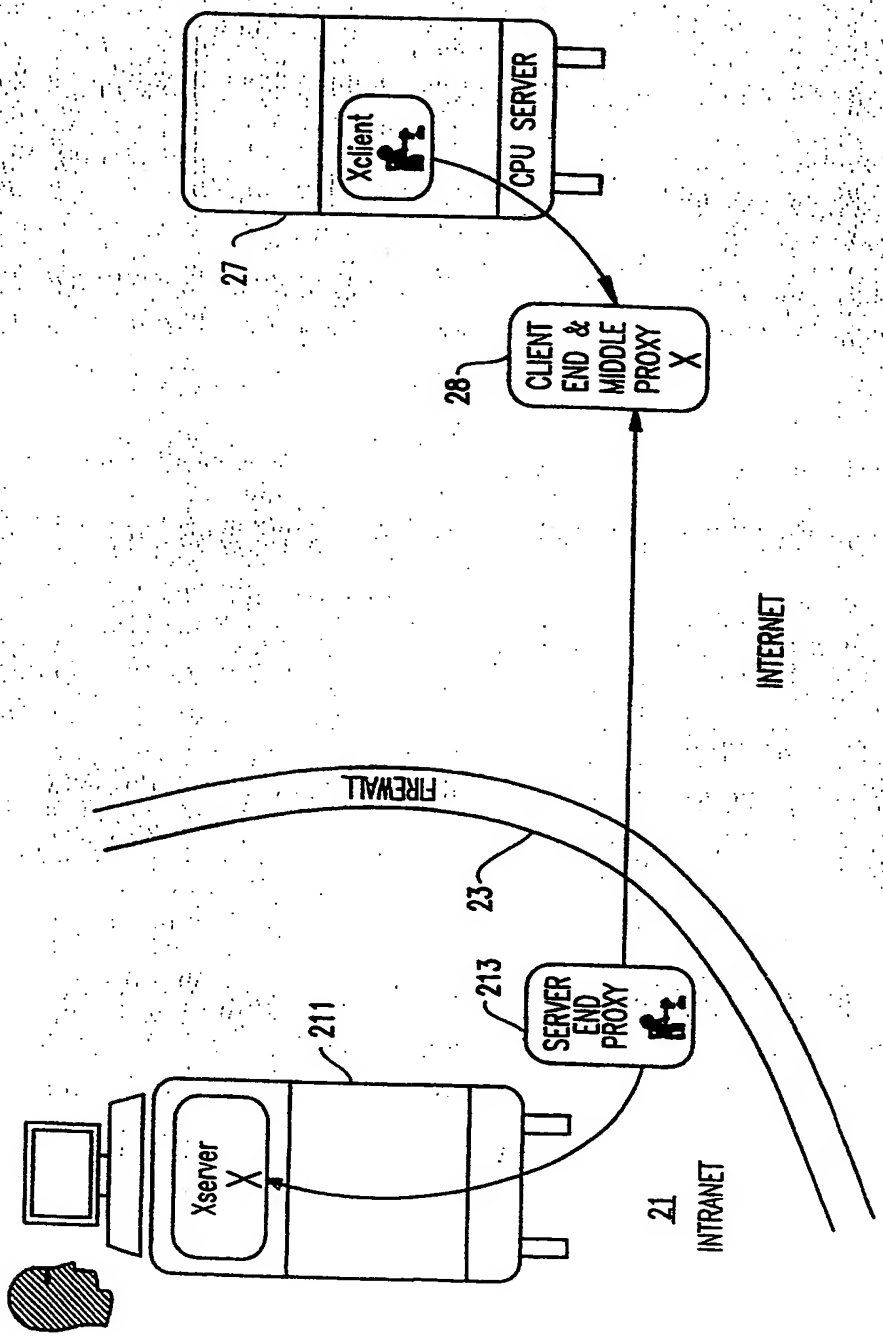


FIG.9

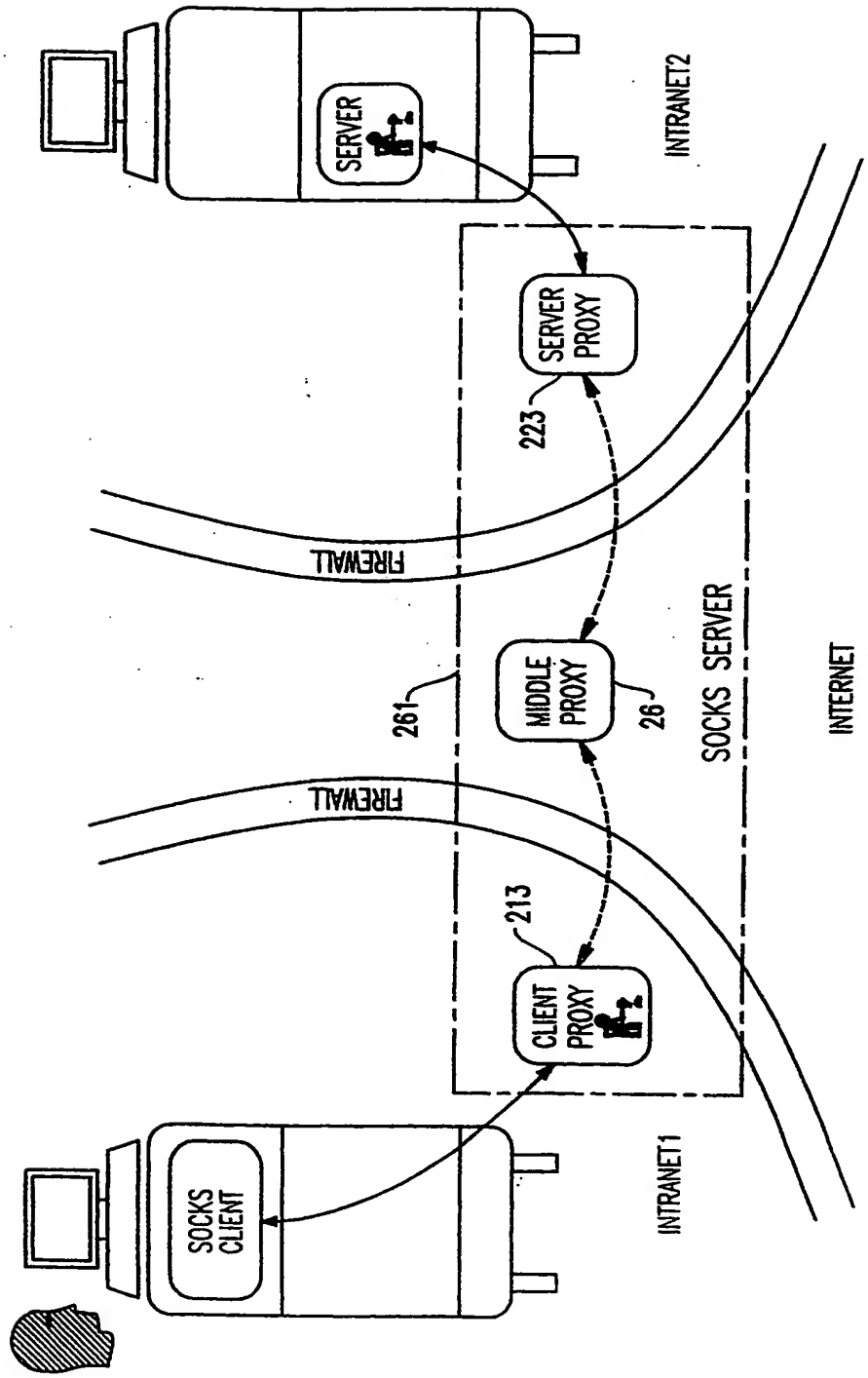


FIG.10

2323757

METHOD AND APPARATUS FOR LIGHTWEIGHT SECURE COMMUNICATION TUNNELLING OVER THE INTERNET

Field of the Invention

The present invention generally relates to packet switched network communications and, more particularly, a method and apparatus which provides the ability to allow a TCP/IP client situated outside of an organization's "firewall" to address a server inside the same firewall, even when the firewall is configured to not allow outside clients to address the inside server.

Background Description

The Internet is a collection of networks throughout the world which facilitates the sharing of resources among participating organizations, including government agencies, educational institutions and private corporations. These networks use the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite and share a common address space. Thus, computers on the Internet use compatible communications standards and share the ability to contact each other and exchange data. Users of the Internet communicate mainly via electronic mail (e-mail), via Telnet, a process that allows users to log in to a remote host, and via implementations of the File Transfer Protocol (FTP), a protocol that allows them to transfer information on a remote host to their local site.

Security is a major concern when connecting a network, such as a local area network (LAN) to the Internet. One of the more important concerns is intruders attempting to gain access to local hosts. A common method for preventing these types of intrusions is to install a so-called "firewall" which is a secure single point of attachment to the Internet. This single point of attachment takes the form of a firewall host which allows only certain traffic to pass through as specified by the firewall administrator. In a typical firewall host implementation, a user wanting to transfer a file on a host in the LAN to an external host via the Internet first transfers the file to the firewall host and then logs into the firewall and transfer the file to the external host. While this procedure provides a high level of security for a single user, maintaining security becomes difficult as the number of users requiring access to this host increases. For general information on firewalls, see

William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley (1994).

A transport layer proxy architecture, called SOCKS, was created in an attempt to minimize security problems while allowing access by a large number of users. See, for example, David Koblas and Michelle R. Koblas, "SOCKS", *UNIX Security Symposium*, USENIX Association (1992), pp. 77-83, and Ying-Da Lee, "SOCKS: A protocol for TCP proxy across firewalls", http://www.socks.nec.com/socks4.protocol, and M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones, "SOCKS Protocol Version 5", ftp://ds.internic.net/rfc/rfc1928.txt. In a transport layer proxy architecture, one end system behind the firewall, which is called the client, initiates a session by making a connection to the proxy, which can be thought of as residing on the firewall. The client and proxy use the connection to exchange messages negotiating session setup information such as authentication or proxy request (e.g., the foreign host to connect to for a firewall proxy or the URL (Uniform Resource Locator) to fetch for an HTTP (Hypertext Transfer Protocol) proxy). The proxy then carries out the request, commonly opening a connection to another end-system, typically outside the firewall, which is called the server, as directed by the client. The proxy may exchange session setup information with the server over the connection. After session setup has been completed on both connections, the proxy begins to copy data back and forth between the two connections and does not delete from, add to, or alter the information flowing between the hosts (although it may silently keep a copy of the information, as in the case of HTTP caching proxies).

Often, an employee inside an organization wishes to allow an "outside" client to address his or her "inside" server. In this case, since the employee trusts the outside client, he or she may wish to bypass the controls put in place on the firewall so that the trusted outside client can address the trusted inside server.

Summary of the Invention

It is an object of the present invention to provide a technique which alleviates the above drawbacks.

According to the present invention we provide a packet switched network communications system comprising: a first network including at least one server running a server application; a second network

including at least one client running a client application; a first firewall guarding computer resources of one of the first and second networks and including a software application that enables the first firewall to make connections from inside to outside the first firewall; a server end proxy and a server application that are mutually addressable; a client end proxy and a client application that are mutually addressable; and a middle proxy outside the first firewall and in an untrusted network between the first and second networks, the server end proxy and the client end proxy each making connections to the middle proxy through the first firewall and the middle proxy connecting the connections from the server end proxy and the client end proxy to establish a pass through communication tunnel between the client and the server.

Further, according to the present invention, we provide, in a packet switched network communications system including a first network including at least one server running a server application, a second network including at least one client running a client application, a first firewall guarding computer resources of one of the first and second networks and including a software application that enables the first firewall to make connections from inside to outside the first firewall, a server end proxy addressable by the server application, a client end proxy addressable by the client application, and a middle proxy outside the first firewall and in an untrusted network between the first and second networks, a method of connecting the server end proxy and the client end proxy to the middle proxy through the first firewall and the middle proxy connecting the connections from the server end proxy and the client end proxy to establish a pass through communication tunnel between the client and the server, the method comprising the steps of: starting the middle proxy and waiting for a first connection from an end proxy; starting the client end proxy and opening a connection to the middle proxy by sending client setup information to the middle proxy; storing by the middle proxy the end proxy setup information and then waiting for a second connection; starting the server end proxy and opening a connection to the middle proxy by sending end proxy setup information to the middle proxy; pairing by the middle proxy the connections of the client end proxy and the server end proxy and transmitting server and middle proxy setup information to the client end proxy and client and middle proxy setup information to the server end proxy; and the middle proxy thereafter acting as a pass through between the client end and server end proxies.

According to a preferred embodiment of the invention, there is provided a lightweight secure tunnelling protocol or LSTP which permits communicating across one or more firewalls by using a middle server or proxy. More particularly, the basic system uses three proxies, one middle proxy and two end proxies, to establish an end-to-end connection that navigates through two firewalls. In this configuration, a server behind a first firewall and a client behind a second firewall are interconnected by an untrusted network (e.g., the Internet) between the firewalls. A first inside firewall SOCKS-aware end server-side proxy connects to the server inside the first firewall. The client inside the second firewall connects to a second inside firewall SOCKS-aware client-side end proxy. Both server-side and client-side end proxies can address a third proxy (called a middle proxy) outside the two firewalls. The middle proxy is usually started first, as the other two proxies (server and client end proxies) will initiate the connection to the middle proxy some time after they are started. Since the middle proxy is mutually addressable by both inside end proxies, a complete end-to-end connection between the server and client is established. It is the use of one or more middle proxies together with an appropriate protocol like LSTP that establishes the secure communications link or tunnel across multiple firewalls.

Brief Description of the Drawings

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure 1 is a block diagram illustrating the typical interaction between a client application and a server application when the server is behind a firewall;

Figure 2 is a block diagram illustrating the typical interaction between a client application and a server application when the client is behind a firewall;

Figure 3 is a block diagram illustrating a typical network configuration between two companies or organizations each having networks behind firewalls;

Figure 4 is a block diagram illustrating the three types of proxies used according to the invention to construct a secure communications channel or tunnel between two companies or organizations;

Figure 5 is a data flow diagram illustrating the interaction between the client, middle and server proxies shown in Figure 4;

Figure 6 is a table summarizing the Lightweight Secure Tunnelling Protocol (LSTP) according to a preferred embodiment of the invention.

Figure 7 is a flow diagram of the process performed on an end proxy;

Figure 8 is a flow diagram of the process performed on a middle proxy;

Figure 9 is a block diagram illustrating an alternative embodiment of the invention where the server proxy connects to the client proxy over a single firewall; and

Figure 10 is a block diagram illustrating another alternative embodiment of the invention in which SOCKS-aware clients allow secure communications over two firewalls.

Detailed Description of Preferred Embodiments of the Invention

Referring now to the drawings, and more particularly to Figure 1, there is shown two networks 11 and 12 separated by a firewall 13. The firewall 13 is used to guard the first network 11 against malicious activity originating from outside the firewall. Network 11 is, in this illustration, Company A's private network, and network 12 is typically the Internet. In this example, network 11 is represented by a server 111 running a server application and a client 112 running a client application. The client application running on client 112 behind the firewall 13 can address the server application running on server 111, but a client application running on client 122 outside the firewall 13 cannot address the server application running on server 111 since this connection is blocked by the firewall. That is, the purpose of the firewall 13 is to guard the computer resources of Company A, in this case, network 11 which may comprise many servers and clients connected together on a local area network (LAN).

In Figure 2, there is shown a similar arrangement except that there is a server 121 running a server application in network 2. As in Figure 1, the client application running on client 112 can still address the server application running on server 111. If enabled to allow connections from inside to outside, the firewall 13 will also allow the client application running on client 112 to connect to the server application running on server 121 outside the firewall 13. The common software package called SOCKS mentioned above enables firewalls to make connections from inside to outside as shown in Figure 2.

Figure 3 again shows two networks but this time the second network 14 is Company B's private network which is behind a second firewall 15. Thus, firewall 15 is designed to protect Company B's computer resources from malicious activity originating from outside firewall 15. In this illustration, a client application running on a client 142 behind firewall 15 may attempt to address the server application running on server 111 behind firewall 13 via the Internet 12. However, while firewall 15 may have the SOCKS capability to allow client application running on client 142 to connect outside the firewall 15, firewall 13 prevents the connection to the server application running on server 111.

Often, an employee inside an organization wants to allow an "outside" client application to address an "inside" server; e.g., to allow the client application running on client 142 to address the server application running on server 111 in Figure 3. In this case, the employee trusts the outside client application and wishes to bypass the controls put in place on their company's firewall that prevent the trusted outside client from addressing the inside server. This invention provides a solution for this situation.

The invention will be described, without loss of generality, in terms of an implementation in the X Windows System. The X Windows System is a standardized set of display-handling routines, developed at MIT for UNIX workstations, that allow the creation of hardware-independent graphical user interfaces (GUIs). In the example described first, two firewalls are addressed. The initial implementation builds on the SOCKS package which enables SOCKS-aware programs inside a SOCKS gateway to connect to servers outside the SOCKS gateway.

Figure 4 shows the three types of proxies used to construct a secure tunnel and their placement in the network configuration according to the present invention. Network 21, Company A's private network or intranet, is protected by firewall 23, and network 22, Company B's private network or intranet, is protected by firewall 25. Behind firewall 23 is an X-server 211, part of Company A's private network, and behind firewall 25 is an X-client 222, part of Company B's private network. Both firewalls 23 and 25 have SOCKS capability to allow "inside" clients to connect to "outside" servers. The X-client 222 has within its addressable domain behind Company B's firewall 25 a client end proxy 223 that has the ability to listen for X protocol. The client end proxy 223 appears as a local X-server to the X-client 222, so no modifications are needed to the X-client 222.

A similar situation exists behind Company A's firewall 23 where a server end proxy 213 exists within the addressable domain of the X-server 211. The server end proxy 213 is able to connect to the X-server 211 just as a real X-client would. The server end proxy 213 appears as a local X-client to the X-server 211 so, again, no modifications are needed to the X-server 211.

A middle proxy 26 is started first, as the end proxies will initiate connections to the middle proxy. The client end proxy 223 and the server end proxy 213 make use of existing capability (e.g., SOCKS) to make requests through a firewall from the inside to the outside. Since the middle proxy 26 is mutually addressable by both end proxies (using SOCKS on each firewall), a complete end-to-end connection between the X-client 222 and the X-server 211 can be established through the middle proxy 26.

The middle proxy 26, which appears as a server to both the client end proxy 223 and the server end proxy 213, is a key feature of the invention. As such, both the client end proxy 223 and the server end proxy 213 can address the middle proxy 26 through their respective firewalls 25 and 23. For cascaded or multiple middle proxies, the middle proxies may actually address other middle proxies as opposed to being addressed by end proxies. The initial connection is made using the standard TCP/IP connection mechanism. Each established connection, no matter which program initiated it, is a TCP/IP connection and is therefore duplex. This invention provides a Lightweight Secure Tunnelling Protocol (LSTP) which is used on top of TCP/IP to provide for

proper sequencing of tunnel management events. LSTP is "spoken" between the client end, server end and middle proxies not just during tunnel construction, but through out the entire tunnel lifetime.

The triggers for the end proxies 213 and 223 to initiate a connection to the middle proxy 26 is manually controlled by someone who has access to the computer where the end proxies 213 and 223 are running. The end proxies 213 and 223 can establish a connection to the middle proxy 26 anytime after the middle proxy is started. The middle proxy 26 will receive and store the setup information sent to it by the first connecting end proxy.

When the middle proxy has two matching connections, one from a client end proxy 223 and one from a server end proxy 213, the middle proxy 26 will join the two connections and act like a transparent pipe, effectively establishing a connection between the two end proxies. From this time forward, the middle proxy 26 is in a pass through mode, and one end proxy initiates a security handshake with the other end proxy to secure the tunnel.

The X-client 222 can now initiate a connection to and passes data to the client end proxy 223 just as if it were connected directly to the X-server 211. The initial data from X-client 222 causes LSTP messages to flow through the tunnel established by the two end proxies 223 and 213 and the middle proxy 26 which then causes server end proxy 213 to initiate a connection to X-server 211. The data from X-client 222 is then passed through the tunnel and presented to the X-server 211. Neither the X-client 222 nor the X-server 211 have any indication that they are not talking directly to each other. Data flows in both directions; from the X-server 211 to the X-client 222 and from the X-client 222 to the X-server 211. At this point, additional clients could connect to the client proxy and use the same or request a new tunnel connection.

To summarize, the server-side end proxy can connect to the inside X Windows System server and the outside middle proxy, and the X Windows System client can connect to the client-side end proxy which can then connect to the outside middle proxy for the X-client. Due to the fact that an established connection is duplex in nature, and due to transitive closure, the X Windows System client can address the X Windows System server as if there were no firewall (i.e., as if they were on the same

addressable network). Those skilled in the art will recognize that the functionality of the end proxies can be increased to allow for other protocols and services. For example, one end proxy could provide both client and server end proxy functionality.

Figure 5 is a data flow diagram illustrating the interaction between the client, middle and server proxies. The process assumes that the middle proxy has been started and it is waiting for the first connection. The client end proxy is started and opens a connection to the middle proxy and sends client setup information to the middle proxy. "Setup information" is a general term describing two pieces of the LSTP protocol. The middle proxy stores the end proxy setup information and then waits for the second connection. The server end proxy is started and opens a connection to the middle proxy, and the server end proxy sends end proxy setup information to the middle proxy. The middle proxy pairs the connections and transmits server and middle proxy setup information to the client end proxy and client and middle proxy setup information to the server end proxy.

Only can communicate when both client and server end proxies independently connect to middle proxy

At this point in the process, the middle proxy ceases any active role in the connection and acts as a pass through between the client end and server end proxies. Once the connection has been established, either one of the end proxies can initiate a security handshake. An algorithm in each end proxy uses the setup information to decide which end proxy initiates the security handshake. In Figure 5, the client end proxy is shown as transmitting a security handshake that is passed to the server end proxy. The server end proxy responds with a security handshake that is passed to the client end proxy. When this security protocol has been accomplished, additional setup information is re-transmitted over a secure line to complete the tunnel construction. Those skilled in the art will recognize that an alternative sequence of events could be used to establish end to end security over the tunnel. With the connection between the client application and the server application completed, and data can securely pass in both directions between the two using a protocol such as the Lightweight Secure Tunnelling Protocol (LSTP) described below. As a result, the client and server applications have effectively had their addressability extended.

The server and client proxies 213 and 223 handle (1) authentication, encryption, and integrity, (2) firewall pass through, and (3) data compression. The middle proxy 26 acts as a two way pipe. The

server end proxy 213 appears as an X client to the X server 211, while the client end proxy 223 appears as an X server to the X client 222. The server and client end proxies usually reside on the same machine as the X server and X client, respectively.

With this general overview, there are several implementation decisions which were made to implement the secure tunnel between the two networks 21 and 22. First, in the example illustrated, X Windows System clients and servers were used on each tunnel end and, as such, the end proxies are customized to listen for and respond to X protocols. Second, the Secure Sockets Layer (SSL) was chosen as the security protocol to secure the tunnel. SSL provides for data integrity, data privacy, and authenticity of the originating parties. Third, SOCKS was chosen as a mechanism to allow proxies to establish connections from inside the firewall to outside the firewall. Fourth, the Lightweight Secure Tunnelling Protocol (LSTP) was developed along with the tunnel to provide a means for formalizing tunnel construction, management, data flow control, and tunnel destruction.

The Lightweight Secure Tunnelling Protocol (LSTP) according to the invention is the protocol used between the client proxy 223 and the middle proxy 26 and between the server proxy 213 and the middle proxy 26 shown in Figure 4. In the preferred embodiment, LSTP includes the following meanings of and sequencing rules for requests and responses used for transferring data between and synchronizing the states of the proxies:

COMMONUNIQUE_INFO - This information allows two end proxies connect at different times to the same middle proxy. The middle proxy knows that these two end proxies should be paired together because they both provided the same common information. The unique information could be used to identify each end proxy user.

TOPOLOGY_EXCHANGE - This is information that describes the topology of the tunnel. Middle proxies append its topology (e.g., name, address, etc.) information to any TOPOLOGY_EXCHANGE it receives and forwards the TOPOLOGY_EXCHANGE downstream to the end proxy. This provides each end proxy with a map of which proxies are participating in the tunnel.

PROPERTY_EXCHANGE - This mechanism allows for end proxies to exchange information about themselves.

CONNECTION_REQUEST - This request allows one end proxy to notify the other end proxy that a client application is requesting tunnel resources to be allocated for use by the client application. Requested resources may include "multiplexed" channels on an existing tunnel connection or new tunnel connections in addition to established tunnel connections.

CONNECTION_ACK and **CONNECTION_NACK** - These responses allow the proxy receiving a CONNECTION_REQUEST to either accept or deny the request for tunnel resources.

SERVICE_BEGIN_REQUEST - This request allows an end proxy to notify the other end proxy that an application is beginning to send data and therefore use the tunnel resources that have been requested and/or allocated.

SERVICE_BEGIN_ACK and **SERVICE_BEGIN_NACK** - These responses allow an end proxy to accept or deny an application's request to begin using resources that have been allocated.

SERVICE_DATA - This message is used to send application data between two end proxies. Each client/server application pair has a unique identifier included in its SERVICE_DATA message to allow multiple applications to multiplex their data over one TCP/IP connection.

SERVICE_DATA_PAUSE - This message allows an end proxy to tell the other end proxy to stop sending application data.

SERVICE_DATA_RESUME - This message allows an end proxy to tell the other end proxy to resume sending application data.

SERVICE_FREE_REQUEST -This request allows an end proxy to notify the other end proxy that an application is done and tunnel resources can be freed.

SHUTDOWN - This allows an end proxy to shut down the tunnel gracefully by notifying the other end proxy.

ERROR - This message allows an end proxy to exchange error information.

The LSTP is summarized in Figure 6. Note that the first three messages are used to manage tunnel setup and administration. Specifically, the setup information is comprised of varying combinations of COMMONUNIQUE_INFO and TOPOLOGY_EXCHANGE LSTP messages and is used to manage tunnel connections. The next six messages are used to manage resources of an existing tunnel as required by applications using the tunnel. The next message, SERVICE_DATA, is used to transport application data between end proxies. The next two messages are used to manage application data, that is, flow control. The next three messages are used to manage clean up of tunnel resources no longer needed by an

application. Finally, the last message is used to manage error conditions.

This Lightweight Secure Tunnelling Protocol (LSTP) was developed to facilitate tunnel resource management and life cycle. Those skilled in the art will recognize that another protocol encompassing similar features and functionality could be created to accomplish the same goal.

The end proxy flow diagram is shown in Figure 7. The process begins by connecting to a middle proxy in function block 701. The end proxy then sends its COMMONUNIQUE_INFO and TOPOLOGY_EXCHAGE setup information to the middle proxy in function block 702. Next, the end proxy receives other proxies COMMONUNIQUE_INFO and TOPOLOGY_EXCHANGE set information from the middle proxy in function block 703. A master end proxy is chosen based on the TOPOLOGY_EXCHANGE setup information in function block 704. If this proxy is the master end proxy as determined in decision block 705, then a security handshake is initiated in function block 706; otherwise, the end proxy waits for the security handshake in function block 707. Once the security handshake is complete in function block 708, the end proxy resends the COMMONUNIQUE_INFO and TOPOLOGY_EXCHANGE setup information over the secured connection in function block 709. Then, in function block 710, the proxy again receives the COMMONUNIQUE_INFO and TOPOLOGY_EXCHANGE setup information over the secured connection. If the end proxy is a client end proxy, as determined in decision block 711, the proxy waits for the local client application to connect in function block 712. When the local client application is connected in function block 713, the connection is setup and managed using the Lightweight Secure Tunnel Protocol (LSTP) in function block 714. If, on the other hand, the proxy is a server end proxy as determined in decision block 711, the proxy waits for the other end proxy to request a connection in function block 715. When the CONNECTION_REQUEST message is received from the other end proxy in function block 716, the connection is setup and managed using the Lightweight Secure Tunnel Protocol (LSTP) in function block 714.

The middle proxy flow diagram is shown in Figure 8. The process begins by checking in decision block 801 whether there is a new connection from a neighbouring proxy. If so, the new connection is accepted in function block 802, and then a determination is made in decision block 803 as to whether a matching COMMONUNIQUE_INFO message is stored from a previous connection. If not, the COMMONUNIQUE_INFO and

base to another platform. In general, an end proxy, middle proxy, and another end proxy could make up a tunnel where each proxy is running on a different hardware/software platform. The end and middle proxies both place relatively low demands on the resources of the computer they are running on.

CLAIMS

1. A packet switched network communications system comprising:

a first network including at least one server running a server application;

a second network including at least one client running a client application;

a first firewall guarding computer resources of one of the first and second networks and including a software application that enables the first firewall to make connections from inside to outside the first firewall;

a server end proxy and a server application that are mutually addressable;

a client end proxy and a client application that are mutually addressable; and

a middle proxy outside the first firewall and in an untrusted network between the first and second networks, the server end proxy and the client end proxy each making connections to the middle proxy through the first firewall and the middle proxy connecting the connections from the server end proxy and the client end proxy to establish a pass through communication tunnel between the client and the server.

2. The packet switched network communications system recited in claim 1 further comprising a second firewall guarding computer resources of the other one of the second and first networks and including a software application that enables the second firewall to make connections from inside to outside the second firewall.

3. The packet switched network communications system recited in claim 2 wherein the server end proxy, the client end proxy and the middle proxy constitute a tunnel having SOCKS server capability, the entire tunnel performing the job of a SOCKS server.

4. In a packet switched network communications system including a first network including at least one server running a server application, a second network including at least one client running a client application, a first firewall guarding computer resources of one of the first and second networks and including a software application that enables the first firewall to make connections from inside to outside the first firewall, a server end proxy addressable by the server application, a client end proxy addressable by the client application,

and a middle proxy outside the first firewall and in an untrusted network between the first and second networks, a method of connecting the server end proxy and the client end proxy to the middle proxy through the first firewall and the middle proxy connecting the connections from the server end proxy and the client end proxy to establish a pass through communication tunnel between the client and the server, the method comprising the steps of:

starting the middle proxy and waiting for a first connection from an end proxy;

starting the client end proxy and opening a connection to the middle proxy by sending client setup information to the middle proxy;

storing by the middle proxy the end proxy setup information and then waiting for a second connection;

starting the server end proxy and opening a connection to the middle proxy by sending end proxy setup information to the middle proxy;

pairing by the middle proxy the connections of the client end proxy and the server end proxy and transmitting server and middle proxy setup information to the client end proxy and client and middle proxy setup information to the server end proxy; and

the middle proxy thereafter acting as a pass through between the client end and server end proxies.

5. The method recited in claim 4 further comprising the steps of:

after pairing by the middle proxy of the connections between the client end and server end proxies, exchanging by the client end and server end proxies security handshakes; and

again exchanging setup information between the client end and server end proxies via the middle proxy over the secured line.

6. The method recited in claim 5 further comprising the step of releasing tunnel resources between the client end and server end proxies when data exchange between the client and server over the tunnel have been completed.

The Patent Office

Application No:	GB 9803074.5	**Examiner:**	Keith Williams
Claims searched:	1-6	**Date of search:**	24 June 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): H4P (PPA, PPEB, PPEC)

Int Cl (Ed.6): H04L 9/00, 12/22, 12/46, 12/66, 29/06, 29/08

Other: Online WPI, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X,E	GB 2318031 A	Secure Computing Corp. - see abstract	1,4
A,E	GB 2317539 A	Secure Computing Corp. - see abstract, Fig. 1	1,4
A	EP 0743777 A2	Sun Microsystems Inc. - see abstract	1,4
X	EP 0713311 A1	Milkyway Networks Corp. - see abstract, Claim 1 (and US 5623601)	1,4
A,E	WO 98/18248 A1	IBM Corp. - see abstract, Claim 1	1,4
X,P	WO 97/16911 A1	IBM Corp. - see abstract, Fig. 3	1,4

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

CPEL0154167P

Text of the First Office Action

After examination, comments are given as follows:

1. Said "communication control session" referred to by claim 9 should be said "control communication session" in claim 1, but claim 9 uses an inconsistent technical term, so claim 9 is not in conformity with the provision of Rule 21, para. three, of the Implementing Regulations of the Patent Law.

2. In claim 12, said "third server" in the expression "a third session between said third server and said one of said at least host" is not mentioned in the application, which should be a "second server", so claim 12 is not in conformity with the provision of Rule 20, para. one, of the Implementing Regulations of the Patent Law.

3. Claims 2-10 and 12-20 refer to claims 1 and 11 respectively, the titles of the subject matters in claims 2-10 and 12-20 are inconsistent with those of the claims as referred to, so claims 2-10 and 12-20 are contrary to the provision of Rule 23, para. one, of the Implementing Regulations of the Patent Law.

Even if the applicant would overcome the aforesaid defects, claims 1-20 are still contrary to the provisions of Article 22 of the Patent Law. The following comments are made based on such hypothesis:

4. Claim 1 seeks protection for a system for communicating data using a data communication session between a user terminal and a host, reference document 1 (GB2323757A, published on September 30, 1998) discloses a tunnel-type network secure communication system used for

communicating data using a data communication session between a user terminal and a host, said user terminal being coupled to a first network and said host being coupled to a second network, said system comprising: a client end proxy (corresponding to a first server of claim 1) coupled to a first network, the client end proxy is equivalent to the local server of the user terminal; a server end proxy (corresponding to a second server of claim 1) coupled to a second network; and a middle proxy (corresponding to the internal firewall 20 of the present application); the middle proxy receives from the server end proxy the control communication session setup information, and receives from the user terminal the data communication session setup information, the data communication session setup information is issued from the user terminal and is used for requesting a data communication session between the user terminal and the server; after the middle proxy receives the data communication setup information, only when the control communication session setup information issued from the server end proxy is received, a tunnel is formed between a server end proxy and a client end proxy and the data communication session is set up (See page 7, line 1 to page 10, line 23 of the description, and Figs. 4 and 5). Thus, it can be seen that reference document 1 discloses all the technical features of claim 1, and the technical solution as disclosed by the reference document and the claimed technical solution of claim 1 pertain to the same technical field and can produce the same technical effect. Therefore, claim 1 does not possess novelty over reference document 1 and hence is not in conformity with the provision of Article 22, para. two, of the Patent Law.

5. Claims 2, 5 and 6 all refer to claim 1, the additional technical features in the characterizing portions thereof have already been disclosed by reference document 1, reference document 1 discloses the following features: setting a firewall between the client end proxy and server end proxy (See page 7, lines 1-9 of the description and Fig. 4); the data

communication session setup information is transmitted from the client end proxy to the server end proxy through establishing the communication control session (See page 8, lines 23-26 of the description); the client end proxy supports multiple data communication sessions between one or more user terminals and one or more hosts (See page 8, lines 31-33 of the description). Thus, it can be seen that claims 2, 5 and 6 are not in conformity with the provision as to novelty of Article 22, para. two, of the Patent Law over reference document 1.

6. The additional technical features in the characterizing portions of claims 3 and 7 are commonly known in the art. For those skilled in the art, the setting of a firewall and the content that the server end proxy supports multiple data communication sessions between one or more user terminals and one or more hosts are quite obvious. Therefore, claims 3 and 7 do not possess prominent substantive features and notable progress over reference document 1 and hence are contrary to the provision as to inventiveness of Article 22, para. three, of the Patent Law.

7. Claim 4 referring to claim 2 further defines that said first firewall has the function of denying all communication control session establishment requests other than those communication controls session establishment requests which are sent to said first server by the second server, in reference document 1, it is a middle proxy that realizes such function (See page 9, lines 6-18 of the description and Fig. 5). Although such function is not accomplished in the firewall of reference document 1, the reference document given an enlightenment of assigning this function to the firewall. Therefore, claim 4 does not possess prominent substantive features and notable progress over reference document 1 and hence is contrary to the provision as to inventiveness of Article 22, para. three, of the Patent Law.

8. The additional technical features in the characterizing portions of claims 8-10 have already been disclosed by reference document 2 (WO9818248A1, published on April 30, 1998), reference document 2 discloses a tunnel apparatus of data communication network including a firewall, the inside interface server within the firewall creates a "control connection" to the outside interface server, this control connection can only be formed under the control of the program running within the firewall and it sends a trusted socket table to the outside interface server, the trusted socket table comprising a port to host address map (See page 4, line 36 to page 7, line 39 of the description and Figs. 1-5). Thus, it can be seen that claims 8-10 do not possess prominent substantive features and notable progress over reference document 1 and hence are contrary to the provision as to inventiveness of Article 22, para. three, of the Patent Law.

9. Claim 11 seeks protection for a method for communicating data using a data communication session between multiple user terminals and at least one host via a first and second server, the steps of this method correspond to the functions of the composing structures of the system in claim 1 one by one. Therefore, based on corresponding reasons and evidences as mentioned above in respect of claim 1, claim 11 is not in conformity with the provision as to novelty of Article 22, para. two, of the Patent Law over reference document 1.

10. Part of the additional technical features of claim 12 have already been disclosed by reference document 1, reference document 1 discloses the data communication session is established via a first session, a second session and a third session (See page 8, lines 5-34 of the description), whereas the content that the data is transferred between the first and second sessions via a first computing thread and the data is transferred between the second and third sessions via the second thread is commonly known in the art and this is obvious to those skilled in the art. Therefore,

claim 12 does not possess prominent substantive features and notable progress over reference document 1 and hence is contrary to the provision as to inventiveness of Article 22, para. three, of the Patent Law.

11. The additional technical features in the characterizing portions of claims 13, 14 and 19 have already been disclosed by reference document 1, reference document 1 discloses the following features: the data transfer in each of the sessions, the transfer between sessions being bidirectional; sending the data communication connection setup information from the client end proxy to the server end proxy, the first and second sessions being established according to said information; and the client end proxy supporting multiple data communication sessions between one ore more user terminals and one or more hosts (See page 8, lines 5-34 of the description). Thus, it can be seen that claim 13 does not comply with the provision as to inventiveness of Article 22, para. three, of the Patent Law over reference document 1, and claims 14 and 29 are not in conformity with the provision as to novelty of Article 22, para. two, of the Patent Law over reference document 1.

12. The additional technical feature in the characterizing portion of claim 15 corresponds to that of claim 4. Therefore, based on corresponding reasons and evidences as mentioned above in respect of claim 4, claim 15 is not in conformity with the provision as to inventiveness of Article 22, para. three, of the Patent Law over reference document 1.

13. The additional technical features in the characterizing portions of claims 16-18 have already been disclosed by reference document 2, reference document 2 discloses the following features: when the outside user sends to the outside interface server a request for connecting to the inside server, whether said request is directed to a trusted socket entry that is currently valid is decided on the outside interface server, if not, the

connecting request is refused, if said request is directed to a trusted socket entry that is currently valid, the connecting request is allowed (See page 2, line 3 to page 3, line 32 of the description). Thus, claims 16-18 do not possess prominent substantive features and notable progress over reference documents 1 and 2 and hence are not in conformity with the provision as to inventiveness of Article 22, para. three, of the Patent Law.

14. The additional technical feature in the characterizing portion of claim 20 belongs to the common knowledge in the art, for those skilled in the art, it is obvious that the server end proxy supports multiple data communication sessions between one ore more user terminals and one or more hosts. Therefore, claim 20 does not possess prominent substantive features and notable progress over reference document 1 and hence is not in conformity with the provision as to inventiveness of Article 22, para. three, of the Patent Law.

For reasons mentioned above, the independent claims and dependent claims of the present application do not possess novelty or inventiveness. In the meanwhile, the description fails to disclose any other substantive contents which are patentable. Therefore, even if the applicant recombines the claims and/or makes further limitation in the light of the disclosure contained in the description, the application does not have the prospect of being granted. If the applicant cannot produce adequate reasons why the application does possess inventiveness within the time limit for response as specified in the Office Action, the application shall be rejected.

CPEL0154167P

Patent Office of the People's Republic of China

Address : Receiving Section of the Chinese Patent Office. No. 6 Tucheng Road West, Haidian District, Beijing.Postal code: 100088

Applicant	JPMORGAN CHASE BANK			Seal of Examiner	Date of Issue
Agent	China Patent Agent (H.K.) Ltd.				November 7, 2003
Patent Application No.	00810594.4	Application Date	May 17, 2000	Exam Dept.	
Title of Invention	SECURED SESSION SEQUENCING PROXY SYSTEM AND METHOD THEREFOR				

First Office Action

(PCT application entering into the national phase)

1. ☑ Under the provision of Art. 35, para. 1 of the Patent Law, the examiner has made an examination as to substance of the captioned patent application for invention upon the request for substantive examination filed by the applicant.

☐ Under the provision of Art. 35, para. 2 of the Patent Law, the Chinese Patent Office has decided to conduct an examination of the captioned patent application for invention on its own initiative.

2. ☑ The applicant requests that
the filing date May 18, 1999 at the US Patent Office be taken as the priority date of the present application,
the filing date _____ at the _____ Patent Office be taken as the priority date of the present application,
the filing date _____ at the _____ Patent Office be taken as the priority date of the present application.

3. ☐ The following amended documents submitted by the applicant cannot be accepted for failure to conform with Art. 33 of the Patent Law:
☐ the Chinese version of the annex to the international preliminary examination report.
☐ the Chinese version of the amended documents submitted according to the provision of Rule 19 of the Patent Cooperation Treaty.
☐ the amended documents submitted according to the provision of Rule 28 or Rule 41

of the Patent Cooperation Treaty.

☐ the amended documents submitted according to the provision of Rule 51 of the Implementing Regulations of the Patent Law.

See the text portion of this Office Action for detailed reasons why the amendment cannot be accepted.

4. ☐ Examination is conducted on the Chinese version of the initially-submitted international application.

☑ Examination is conducted on the following document(s):

☑ page 1-11 of the description, based on the Chinese version of the initially-submitted international application documents;

page _____ of the description, based on the Chinese version of the annex to the international preliminary examination report;

page _____ of the description, based on the amended documents submitted according to the provision of Rule 28 or Rule 41 of the Patent Cooperation Treaty;

page _____ of the description, based on the amended documents submitted according to the provision of Rule 51 of the Implementing Regulations of the Patent Law.

☑ claim(s) _____ , based on the Chinese version of the initially-submitted international application documents;

claim(s) _____ , based on the Chinese version of the amended documents submitted according to the provision of Rule 19 of the Patent Cooperation Treaty;

claim(s) _____ , based on the Chinese version of the annex to the international preliminary examination report;

claim(s) 1-20 , based on the amended documents submitted according to the provision of Rule 28 or Rule 41 of the Patent Cooperation Treaty;

claim(s) _____ , based on the amended documents submitted according to the provision of Rule 51 of the Implementing Regulations of the Patent Law.

☑ Fig(s) _____ , based on the Chinese version of the initially-submitted international application documents;

Fig(s) _____ , based on the Chinese version of the annex to the international preliminary examination report;

Fig(s) _____ , based on the amended documents submitted according to the provision of Rule 28 or Rule 41 of the Patent Cooperation Treaty;

Fig(s) 1-3 , based on the amended documents submitted according to the provision of Rule 44 of the Implementing Regulations of the Patent Law.

This Page Blank (u

5. ☑ The following reference document(s) is/are cited in this Office Action (its/their serial number(s) will continue to be used in the subsequent course of examination):

Serial No.	Number or Title(s) of Document(s)	Date of Publication (or filing date of interfering application)
1	GB2323757A	Date September 30, 1998
2	WO9818248A1	Date April 30, 1998
3		Date
4		

6. Concluding comments on the examination:

☐ On the description:

☐ What is stated in the application comes within the scope of that no patent right shall be granted as prescribed in Art. 5 of the Patent Law.

☐ The description is not in conformity with the provision of Art. 26, para. 3 of the Patent Law.

☑ On the claims:

☐ Claim(s) _____ come(s) within the scope of that no patent right shall be granted as prescribed in Art. 25 of the Patent Law.

☑ Claim(s) 1, 2, 5, 6, 11, 14, 19 has/have no novelty as prescribed in Art. 22, para. 2 of the Patent Law.

☑ Claim(s) 3, 4, 7, 8-10, 12, 13, 15-18, 20 has/have no inventiveness as prescribed in Art. 22, para. 3 of the Patent Law.

☐ Claim(s) _____ has/have no pratical applicability as prescribed in Art. 22, para. 4 of the Patent Law.

☐ Claim(s) _____ is/are not in conformity with the provision of Art. 26, para. 4 of the Patent Law.

☐ Claim(s) _____ is/are not in conformity with the provision of Art. 31, para. 1 of the Patent Law.

☑ Claim(s) 2-10, 12-20 is/are not in conformity with the provisions of Rules 20 to 23 of the Implementing Regulations.

☐ Claim(s) _____ is/are not in conformity with the provision of Art. 9 of the Patent Law.

☐ Claim(s) _____ is/are not in conformity with the provision of Rule 12, para. 1 of the Implementing Regulations.

See the text portion of this Office Action for detailed analysis of the above

concluding comments.

7. Based on the above concluding comments, the examiner deems that
   - ☐ the applicant should make amendment to the application document(s) according to the requirements put forward in the text portion of this Office Action.
   - ☐ the applicant should expound in his/its observations why the captioned patent application is patentable and make amendment to what is not in conformity with the provisions pointed out in the text portion of this Office Action, otherwise, no patent right shall be granted.
   - ☑ the patent application contains no substantive content(s) for which a patent right may be granted, if the applicant has no sufficient reason(s) to state or his/its stated reason(s) is/are not sufficient, said application will be rejected.
   - ☐

8. The applicant should note the following items:

   (1) Under Art. 37 of the Patent Law, the applicant should submit his/its observations within **four** months from the date of receipt of this Office Action; if, without any justified reason(s), the time limit for making written response is not met, said application shall be deemed to have been withdrawn.

   (2) The amendment made by the applicant to said application should be in conformity with the provision of Art. 33 of the Patent Law, the amended text should be in duplicate and its form should conform with the related provisions of the Guide to Examination.

   (3) If no arrangement is made in advance, the applicant and/or the agent shall not come to the Chinese Patent Office to have an interview with the examiner.

   (4) The observations and/or amended text should be sent to the Receiving Section of the Chinese Patent Office by mail or by personal delivery, if not sent to the Receiving Section by mail or by personal delivery, the document(s) will have no legal effect.

9. This Office Action consists of the text portion totalling 4 page(s) and of the following attachment(s):
   - ☑ 2 copy(copies) of the reference document(s) totalling 22 page(s).

Examination Dept. No. 9 Examiner Xiang Lin
9016